



Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation

A joint World Bank Group - GSMA - Secure Identity Alliance Discussion Paper



The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organizations in adjacent industry sectors. The GSMA works with mobile operators on digital identity and authentication through its **M4D Digital Identity** Programme (www.gsma.com/mobilefordevelopment/programmes/digital-identity) and the **Personal Data Programme via Mobile Connect** (www.gsma.com/personaldata/).



The Secure Identity Alliance (SIA) is dedicated to supporting sustainable worldwide economic growth and prosperity through the development of trusted digital identities and the widespread adoption of secure eServices. The Alliance brings together public, private and non-government organizations to foster international collaboration on Digital ID challenges and the issues of data security, citizen privacy, identity, authentication and more. For information about its growing membership and range of activities visit www.secureidentityalliance.org

The World Bank Group launched the Identification for Development (ID4D) initiative in July 2014, with the objective to support progress toward identification systems using 21st century solutions that enable access to services and rights for all. The initiative is focused on addressing the challenge of the 1.5 billion who have no form of official identity, and therefore unable to access services and rights. For more information visit www.worldbankgroup.org/id4d

Discussion Paper prepared by

Julia Clark^a, Mariana Dahan^a, Vyjayanti Desai^a, Marta Ienco^b, Stephanie de Labriolle^c, Jean-Pierre Pellestor^c, Kyla Reid^b, Yolanda Varuhaki^c

^a The World Bank Group, Washington, DC, USA

^b GSMA, London, UK

^c Secure Identity Alliance, Paris, France

© 2016 International Bank for Reconstruction and Development / The World Bank
1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This work is a joint work of The World Bank, GSMA, and Secure Identity Alliance (“the Contributors”). The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Contributors, their Board of Executive Directors, or the governments they may represent.

The Contributors do not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of the Contributors concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Any queries on rights and licenses, including subsidiary rights, should be addressed to the Publishing and Knowledge Division, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.

Photo credits

Front cover:

Man guiding another in using a fingerprint scanner.
© leezsnow.

Woman holds an ID card. ©Sebastien Rieussec/Safran.

Using smartphone. © mihailomilovanovic.

Back cover:

People forming thumbprint. © Digital Storm

Additional:

A boy holds his birth certificate, outside African Development Bank Zanzan II Primary School, in Bondoukou, Côte d’Ivoire.
© UNICEF/NYHQ2011-2489/Asselin.

Fingerprint. © Jose Luis Gutierrez.

A refugee filling an application at the UNHCR registration center in Tripoli, Lebanon.
©Mohamed Azakir / World Bank, _ZAK6881F.

CONTENTS

DISCLOSURE	6
ABSTRACT	7
GLOSSARY OF TERMS	8
1. DIGITAL IDENTITY FOR SUSTAINABLE DEVELOPMENT: OPPORTUNITIES AND CHALLENGES	10
Introduction	10
Digital Identity for Sustainable Development	11
Key Risks and Challenges	14
2. DIGITAL IDENTITY AND THE ROLE OF PUBLIC AND PRIVATE ACTORS	16
The Identity Lifecycle	16
Stakeholders and Roles	22
Digital Identity Ecosystems: Existing Landscape of Public and Private involvement	25
Models for Private Participation in Official Digital ID Systems	28
3. COMMON PRINCIPLES FOR UNLOCKING THE VALUE OF DIGITAL IDENTITY	33
ANNEX: CASE STUDIES	35
Albania - eID and e-Passport	35
Chile - eID and e-Passport	36
Estonia - Mobile eID	37
Finland - Mobile eID	38
India - Aadhaar Unique ID	39
Moldova - Mobile eID	40
Nigeria - National eID	41
REFERENCES	42

LIST OF TABLES AND FIGURES

Box 1 Defining Digital Identity	11
Figure 1 Digital Identity Lifecycle and Key Roles	17
Box 2 Establishing a Minimum Set of Unique Identity Attributes	18
Figure 2 Common Authentication Factors	20
Figure 3 Levels of Assurance	21
Table 1 Key Identity Stakeholders and Roles	24
Figure 4 Examples of Digital Identity Ecosystems	25
Figure 5 Examples of Private Sector Involvement in Official Digital Identity Systems	29

Disclosure

The findings, interpretations, and conclusions expressed in this paper are entirely those of the authors and should not be attributed in any manner to the World Bank, its affiliated organizations, the members of its Board of Executive Directors, or the countries they represent.

Reference to names of firms and commercial products and processes does not imply their endorsement by the World Bank Group, GSMA or SIA.

Citation and the use of material presented in this paper should take into account this provisional character. The paper is work in progress and is being provided to for information purposes only, in order to facilitate the debate on the latest trends and issues in the area of identification systems.

This work builds on past and on-going efforts and is based on the World Bank Group's ID4D Strategic Framework, the GSMA and SIA joint publication "Mobile Identity – Unlocking the Value of Digital Economy", as well as other strategic documents and research produced by the World Bank Group, GSMA and SIA partners. Because it is a work in progress, there could be some inaccuracies in the data presented in this draft and there could be some parts that are either missing or will be revised. Permission to cite any part of this work must be obtained from the authors.

Abstract

The ability to prove one's identity is increasingly recognized as the basis for participation in social, political, economic, and cultural life. Yet at least a billion people in developing countries lack any form of officially recognized ID. This problem disproportionately impacts rural residents, poor people, women, children, and other vulnerable groups in Africa and Asia. Digital identity, combined with the extensive use of mobile devices in the developing world, offers a transformative solution to this global challenge and provides public and private sector entities with efficient ways to reach the poorest and most disadvantaged. This discussion paper, divided into three parts, explores the connection between digital identity and sustainable development. Part I illustrates how the use of digital identity promotes efficiency gains, financial savings, social inclusion and access to basic services and rights, with examples from countries that have adopted digital identity systems. The paper then outlines some of the key risks and challenges that must be overcome, specifically in the areas of political commitment, data protection and privacy, cost, and sustainable business models. Part II of the paper lays out the digital identity lifecycle and the roles of public and private sector players, and suggests some key considerations in the design of business models. Finally, Part III of the paper suggests some common principles—including universal coverage, appropriate and effective design, and privacy and data protection—and enablers for maximizing the potential of digital identity to contribute to sustainable development.

Keywords:

Digital identity, ID4D, mobile, smart card, biometrics, public-private collaboration, business models, common principles.

Glossary of Terms¹

Digital identity	the terminology used throughout this document to refer to a set of electronically captured and stored attributes and credentials that can uniquely identify a person.
Digital identification	the process of validating a person's attributes and characteristics—including uniqueness—in order to establish his or her digital identity.
Digital authentication	the process of verifying a person's digital identity using one or more factors or credentials in order to establish that they are who they claim to be. Authentication is therefore a process of establishing confidence in a person's digital identity.
Functional registrar	an entity created in response to a demand for a particular service or transaction, which may issue identity tokens such as voter IDs, health and insurance records, bank cards, etc. These may be commonly accepted for broader identification purposes, but may not always bestow legal identity.
Identity assurance	the ability to determine, with some level of certainty (Level of Assurance - LoA), that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity.
Identity credential	a mechanism, process, device or document that vouches for the identity of a person through some method of trust and authentication.
Legal registrars of natural persons	entities that carry out registration of vital events (including births, marriages and deaths) or civil identification for the purpose of establishing <i>legal identity</i> .
Mobile identity	an extension of digital identity provided via mobile networks, data and devices.
Proof of legal identity	official, government-issued and recognized identity evidence that includes basic information attesting to the holder's identity, such as name, identity number, place and date of birth, citizenship, marital status, and/or legal relationships.
National digital identity system	a government-supplied national system that provides digital identities based on identity attributes defined by national law.
Unique identification number (UIN)	a number that uniquely identifies an individual and can be used to link an identity across databases and systems in both the public and private sector. National identity providers may issue a UIN to citizens and residents for their lifetime.

1. Based on key definitions laid out in the World Bank's ID4D Strategic Framework and as agreed with GSMA and SIA. Other sources: Vanderabeele, C. and Lao, C., 2007. *Legal Identity for inclusive Development*. ADB; World Bank 2014; Harbitz, M. and Kentala, K., 2015. *Dictionary for Civil Registration and Identification*. IDB; Gelb, A. and Diofasi, A., 2015. *Scoping Paper on Identification and Development*. Center for Global Development.

ROYAUME DE CÔTE D'IVOIRE

ETAT CIVIL

EXTRAIT

du Registre des actes de l'Etat Civil pour l'année

Le 20 du 10/10/2009 du Registre

Centre TEAPLEU

Le 20 du 10/10/2009 est né 1.

A BOUAFLOU

Fil^m de 1.

Nationalité 1.

et de 1.

Nationalité 1.

E 18

MENTIONS (éventuellement) : NEANT

Marié le _____ à _____

Avec _____


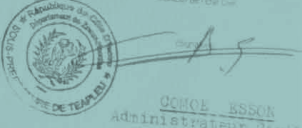
Mariage dissous par décision de divorce en date du _____

Décédé le _____ à _____

Certifié le présent extrait conforme aux indications portées au registre

Délivré à TEAPLEU le 23 NOVEMBRE 2009

L'Officier de l'Etat Civil

COMCE BSSOR
Administrateur Civil

1

Digital Identity for Sustainable Development: Opportunities and Challenges

Introduction

Over 1.5 billion people in the developing world lack any form of officially recognized identification, either paper or electronic-based.² This identity gap is a serious obstacle for participation in political, economic, and social life—without a secure way to assert and verify her identity, a person may be unable to open bank account, vote in an election, access education or healthcare, receive a pension payment, or file official petitions in court.³ Furthermore, poor identification systems mean that states will have difficulty collecting taxes, targeting social programs, and ensuring security. Achieving inclusive development therefore requires a sustained effort to address the world’s identity gap, as reflected in the new Sustainable Development Goals (SDGs).

Much of this effort will be undertaken by national governments and supported by development partners and the donor community. However, given the role that private firms play in the digital identity ecosystem, we are also likely to see evolving models of public-private partnerships to build and strengthen identification in poor countries. In particular, there is significant scope for private sector innovations in new technologies to strengthen the ability of remote or vulnerable

populations to access key services. Yet with this potential come important challenges, and both public and private stakeholders must work together to ensure that digital identity systems are effective, secure, inclusive and trustworthy.

The prospect of increased public-private collaboration to provide digital identity for sustainable development creates the need for a deep analysis of the benefits and challenges of various models of cooperation. This paper is a first step toward meeting this need and setting the scope for future work and further analysis. It begins with Part I by describing the identity gap and the potential benefit of digital identity for a variety of development outcomes—financial inclusion, healthcare, women’s empowerment, service delivery, and governance—as well as key risks and challenges. Part II then discusses the digital identity lifecycle, relevant stakeholders, and examples of digital identity ecosystems and public-private cooperation. Informed by this analysis, Part III lays out a preliminary set of principles for creating digital national identity systems. We hope that these will serve as the basis for further discussion and adoption among a wide range of stakeholders.

2. The WBG ID4D global dataset, as of January 2016. This number is an initial broad estimate based on available information for 198 countries. For countries where there are no reliable and timely data on people in possession of IDs available from government web sites or reports estimates are produced using data from other foundational or functional registers, mainly birth registration data and data from the electoral registers.

3. Gelb and Clark, 2013; Gelb and Diófasi, 2015.

Digital Identity for Sustainable Development

Over one and a half billion people in developing countries lack any form of officially recognized ID.⁴ The problem disproportionately affects children and women from poor rural areas in Africa and Asia. This is a critical stumbling block to economic growth and sustainable development, as the ability to prove one's identity is the basis for participation in modern social, political, and economic life.⁵ In order to address this gap, the 2030 Agenda for Sustainable Development has declared provision of official identity as a proposed target (#16.9) and a key enabler necessary to achieve many other SDGs.⁶

Digital identity provides a potentially transformative solution to this global challenge by offering countries

the ability to leapfrog the development of paper-based systems and rapidly establish robust identification infrastructure. Digital identity (see Box 1) already underpins many public and private sector interactions and transactions in both the real and virtual worlds and can leverage the extensive use of mobile devices in developing countries. When digital identity systems are available, they have the potential to produce huge savings for citizens, government, and businesses; increase transparency and accountability; and drive innovation in service delivery. For example, a global survey conducted by Boston Consulting Group⁷ finds that digital identity systems create gains in efficiency and convenience that could save taxpayers up to \$50 billion per year globally by 2020.⁸

BOX 1

Defining Digital Identity

A **Digital identity** is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A **digital identity system** refers to the systems and processes that manage the lifecycle of individual digital identities.

A person's digital identity may be composed of a variety of attributes, including **biographic data** (e.g., name, age, gender, address) and **biometric data** (e.g., fingerprints, iris scans, hand prints) as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual. When these data are collected and verified, they can be used to **identify** a person by answering the question "*who are you?*". These attributes, along with **credentials** issued by the service provider (e.g., unique ID number, eDocument, eID, mobile ID) can then also be used as **authentication factors** to answer the question "*are you who you claim to be?*". The attributes and authentication factors used in a digital identity may vary from one context or country to the next depending on the type of identity system.

4. World Bank Group, Identification for Development (ID4D) Strategic Framework, Jan 2016

5. Gelb and Clark, 2013.

6. Dahan and Gelb, 2015.

7. Boston Consulting Group, 2013.

8. SIA eGov study, based on analysis from Boston Consulting Group, 2013.

In addition to providing proof of identity (as do paper-based forms of ID), digital ID has the potential to provide public and private sector entities with new and efficient ways to reach and serve their populations, especially the poorest and most disadvantaged. Specifically, the evidence suggests that well implemented digital identification systems can have a significant positive impact on financial inclusion, gender equality, access to health services and social safety nets, and governance.⁹

Financial and Economic Inclusion: Fewer than half of all adults in the poorest 40 percent of households have a bank account. Approximately 375 million unbanked adults in developing countries (18 percent) are prevented from obtaining one because they lack the necessary ID documentation.¹⁰ In addition, many countries now require that pre-paid SIM cards only be activated when registered with a proof of identity; those who lack this ID could be denied access to mobile communication, further exacerbating digital, social and financial exclusion. Accessible, robust, and verifiable ID systems can facilitate the Know Your Customer (KYC) requirements of providers and expand the use of financial services. For example:

- The Reserve Bank of India approved the use of the Aadhaar identification number issued by the Government of India as proof of identity to meet the regulatory KYC requirements of Jan-Dhan basic savings accounts. Approximately 200 million bank accounts have now been opened using Aadhaar.¹¹
- In Pakistan, the national mandate to register and verify SIM cards against the NADRA database allowed branchless banking operators to meet KYC requirements and extend services to SIM registrants remotely.

Gender Equality: Women are less likely to have access to a personal identification than men due to economic and social barriers. As a result, they are less likely to be able to assert their rights over assets (e.g. property, finance) and access public and private benefits and services including welfare payments, healthcare, and

financial services (e.g., without ID to open a bank account, cash transfers targeted to women may be deposited in a household account and thus more likely to be coopted or misused). Increasing the identification of women can improve their inclusion and autonomy. For example:

- Using NADRA's national ID database, Pakistan was able to provide direct cash transfers to women for the first time. As a result, households spent more on nutrition and children's education, and women's participation in household decision making increased.¹²
- After a drought increased food insecurity in northern Malawi in 2006, the Dowa emergency cash transfer program (DECT) was able to provide benefits directly to female heads of household using biometrics and a smartcard.¹³

Access to Health Services: In order to increase access to health services and universal coverage, countries must be able to identify potential beneficiaries of specific health benefits and services (immunizations, insurance, etc.). Additionally, digital ID and vital statistics systems based on civil and population registries (CRVS) can help monitor health targets and track service delivery including vaccinations, HIV/AIDs and TB treatment.¹⁴ For example:

- India and Gabon are implementing national health insurance plans that authenticate beneficiaries using fingerprints and smartcards at points of service.
- In Benin and Nepal, the Vaxtrac program, piloted by the Gates Foundation, uses portable enrollment stations and biometrics to establish a mobile vaccination registry that can uniquely identify patients and ensure continuity of treatment.¹⁵
- In Pakistan, Ghana, and Tanzania, mobile operators are facilitating data collection for CRVS through piloting mobile birth notifications, and are exploring how these can link to maternal and child health services.

9. See the World Bank's ID4D Strategic Framework (2016) for a thorough discussion of these benefits as well as potential risks and challenges to developing inclusive and robust identity systems.

10. Global Findex database: <http://www.worldbank.org/en/programs/globalfindex>

11. <http://www.pmjdy.gov.in/home>

12. Dahan and Hanmer, 2015.

13. Gelb and Decker, 2011.

14. SIA, 2015.

15. Gelb and Clark, 2013.

Social Safety Nets: Accurate identification of the poor and vulnerable makes it possible for social protection programs—including those providing humanitarian and emergency relief—to reach beneficiaries efficiently, securely, and conveniently through digital transfers. For example:

- India’s fuel subsidy program provided cash transfers to Aadhaar-linked bank accounts for the purchase of liquefied petroleum gas cylinders, which saved the government approximately US\$ 2.2 billion in 2014/5.
- Following devastating floods in 2010, Pakistan was able to target relief to affected areas using NADRA’s robust database. Through the Watan card program, the government issued pre-loaded VISA payment cards to 1.5 million families.¹⁶

Governance: Digital identity systems improve government efficiency, accountability and transparency. Through online transactions and other e-services, digital ID systems reduce operational costs

and the corruption and theft occurring in paper-based systems, where entitlement payments are siphoned off from their intended recipients. Authentication protocols based on national identity registers contribute to make government institutions more efficient, accountable, and transparent. For example:

- In Nigeria, biometrically enrolling civil servants through its Integrated Personnel and Payroll Information System saved approximately US\$74 million in the first phase and eliminated 43,000 ghost workers and “double dippers.”
- Biometric identification and mobile phones have been used for monitoring employee attendance. In India and other countries, for example, they have been used to reduce teacher absenteeism.
- In Argentina, the government’s modernized digital identity system linked 13 public databases and distinct ID registries for a savings of US\$104 million in reduced leakage and tax evasion.¹⁷



16. Barnwal, 2015.

17. Gelb and Clark, Ibid.

Key Risks and Challenges

Despite the potential benefits of digital identity for development, efforts to build official identification systems may face a number of challenges, including political complexity, lack of up-to-date legal framework and issues related to data protection, privacy, cost, and sustainability. In order to create and maintain effective systems that are secure, robust, and trusted, actors must work to mitigate these risks.

Political context: Creating an identity system is a complex political process. First, issuing legal identity documents is often coupled with the sometimes-contentious process of determining who is eligible and has access to particular rights and entitlements. Stakeholders need to plan carefully to ensure that identity systems are inclusive and easy to access. Additionally, most countries already have some identification systems in place and may face resistance from actors who have no incentive to change. The creation of a national identity system (digital or otherwise) therefore requires a unified vision and approach that can overcome the common fragmentation of identity by ministries, departments, regions, or donor-funded projects related to identification. To mitigate these risks, stakeholders should¹⁸

- ✓ Assess the existing components of a country's identity infrastructure—including legal and functional identity cards, national registers, and each agency's processes and workflows related to identification services etc.—even if they are not (yet) being used in a digital context. This should include an evaluation of existing laws and identity management practices that may help or hinder access to identification for vulnerable groups.
- ✓ Work to build strong political commitment among relevant stakeholders to guide program design and implementation. This requires including relevant ministries and other stakeholders from the beginning of the process, and working to align the incentives of various actors to support and adopt the new system.

- ✓ Create or revise legislation and internal procedures governing program implementation to (a) provide holistic guidance to government ministries, issuers, and users, (b) minimize the risks of duplication, overlapping or conflicting mandates, technology incompatibility, (c) ensure adequate protection of individual rights, monitoring, and enforcement, and (d) minimize security risks (e.g., cyber attacks) to identity infrastructure, systems and data. Legal frameworks for data collection and storage that were designed for non-digital, non-integrated systems may have to be significantly revised.

- ✓ Create or revise legislation and internal procedures to avoid excluding or deterring vulnerable populations (e.g., women, minorities, migrants and refugees, orphans, etc.) from accessing identity services in law or in practice.

Data Protection and Privacy: Countries that choose to adopt digital identity systems must have robust legal and technical frameworks for data protection and privacy. Missteps in handling citizen data can erode trust in government and decrease the value of the system, threatening revenues and the efficiency gains derived from personal data applications. A recent study estimated that in 2020 alone, two-thirds, or \$480 billion, of the potential value of digital ID in the European Union would be at risk if personal data are not trusted.¹⁹ To mitigate these risks, stakeholders should

- ✓ Establish a harmonized, transparent, and cohesive legal framework for the collection, management, protection, and use of personal data, under the consultation of public and private service providers and citizens. Critically, governments should update existing privacy frameworks in the context of planned and potential future uses of digital ID services.
- ✓ Establish clear and well-publicized procedures for citizen redress in the case of errors or in the event that the security of a person's identity is compromised.

¹⁸ For an elaboration of many of these risks, see World Bank, 2016.

¹⁹ GSMA and SIA, 2014.

- ✓ Build authentication and service delivery systems that use a minimal amount of contextualized data to protect user privacy, and give citizens more oversight over how their data is viewed and access.

Cost and sustainable business models: Creating a digital identity system is a costly project that may require extensive investment in building or updating infrastructure and technology. Discussions with key stakeholders about technology choices and business models—including ways to accelerate national and regional deployment and uptake—are pivotal for avoiding unforeseen costs and ensuring that identity systems can grow efficiently to meet future needs. For example, possible “vendor lock-in” situations can increase costs, reduce flexibility and sustainability, limit market competition, and/or result in an unsuitable system design. Local context and capacity vary, including prior experiences implementing sustainable and appropriate ICT systems, and may necessitate different business models and digital identity solutions. To mitigate these risks, stakeholders should

- ✓ Develop a financial model that details expected costs and potential revenue streams (e.g., additional services) that could help offset the cost of developing a digital identity system. This may include public-private partnerships (PPPs) in which the private sector contributes significant financial capital to a project, as well as support from the donor community.

- ✓ Develop robust ICT procurement guidelines, open standards, and common frameworks to avoid vendor or technology lock-in and enable an array of public and private sector actors (government agencies, businesses, and citizens) to participate in the ID ecosystem. A competitive, open process and smart technology choices will contribute to efficiency and cost savings.

- ✓ Design digital infrastructure appropriate for the context, including strategies to reach remote areas and ensure “last mile connectivity.” Off-line solutions can complement the absence or loss of on-line connectivity.²⁰

- ✓ Ensure the technical capacity of government agencies, private sector and other stakeholders in the digital identity ecosystem (including end-users) to operate and maintain new systems and devices. Global standard setting bodies, identity organizations, and donors can assist countries by providing technical assistance and capacity building to ensure that technology choices are sustainable and that the benefits of digital technology are accessible by the poor and disenfranchised.

20. SIA, 2015.

2

Digital Identity and the Role of Public and Private Actors

The digital identity ecosystem is increasingly complex, with a wide range of identity models and actors with diverse responsibilities, interests, and priorities. This section begins by describing the identity lifecycle and discussing the roles that key stakeholders play in this cycle. It then looks at the relationship between public

and private identity and the different types of identity ecosystems that currently exist, including centralized, federated, and open market models. Finally, it focuses on potential business models for public-private cooperation to create national digital identity systems.

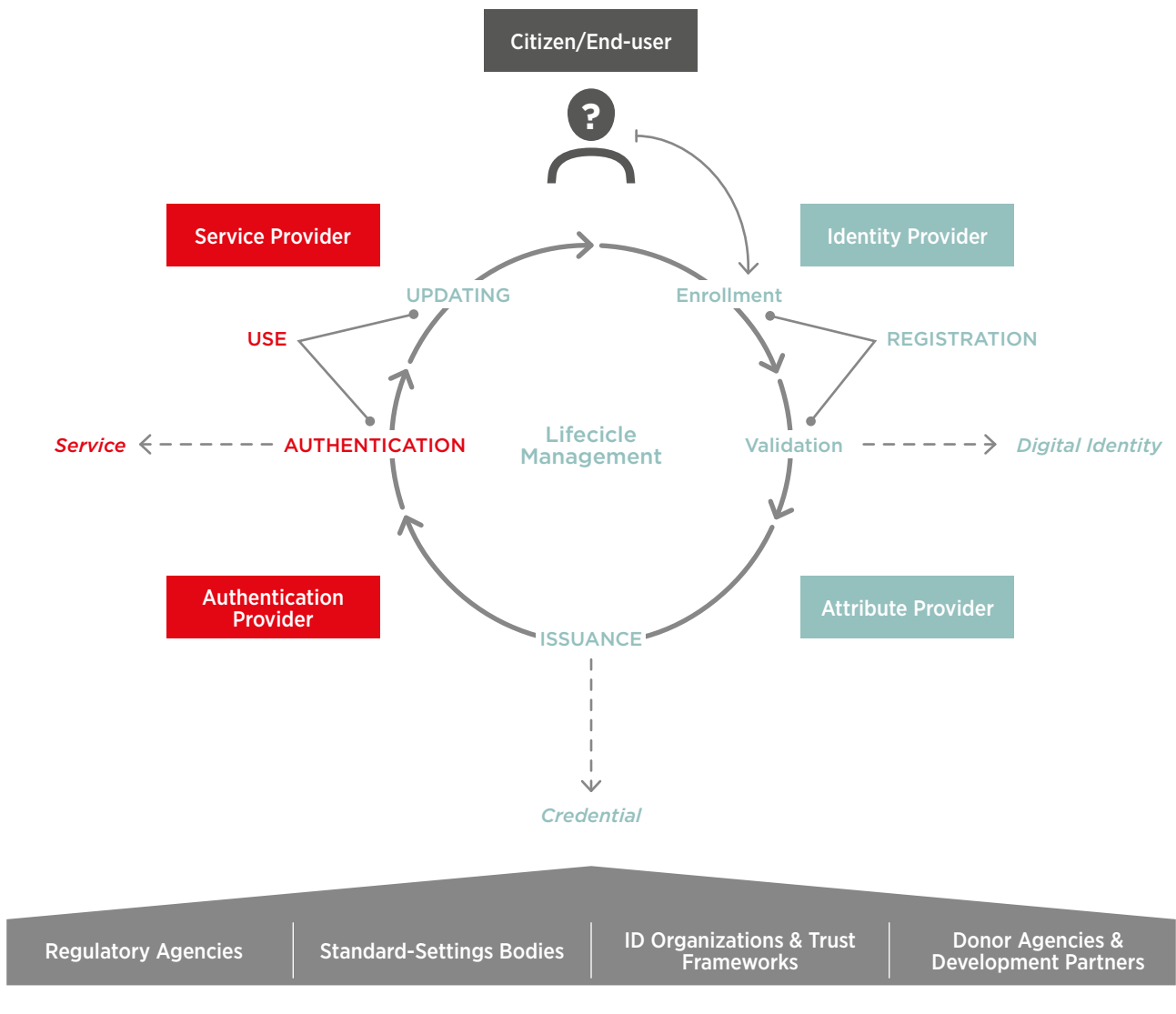
The Identity Lifecycle

Digital identities are created and used as part of a lifecycle that includes three fundamental stages: (a) **registration**, including enrollment and validation, (b) **issuance** of documents or credentials, and (c) **authentication** for service delivery or transactions. Identity providers also engage in ongoing **management** of the system, including updating and revocation or

termination of identities (see Figure 1 below). This section describes each stage and then discusses how the protocols that an identity provider uses during registration and authentication determine the system's **level of assurance** (i.e., how secure and trustworthy it is). The following section discusses the primary stakeholders involved throughout the identity lifecycle.

FIGURE 1 Source: Authors' analysis, based on World Bank, 2014 and GSMA and SIA joint white paper, 2014.

Digital Identity Lifecycle and Key Roles



Registration

Enrollment. Registration is the most important step in creating a digital identity. The process begins with *enrollment*: capturing and recording key identity attributes from a person who claims a certain identity, which may include biographical data (e.g., name, date of birth, gender, address, email), biometrics

(e.g., fingerprints, iris scan) and an increasing number of other attributes. Which attributes are captured during this phase and the method used to capture them have important implications for the trustworthiness of the identity (see the discussion of levels of assurance below) as well as its utility and interoperability with other domestic and international identity systems (see Box 1).

Validation. Once a person has claimed an identity during enrollment, this identity is then validated by checking the attributes presented against existing data. The validation process establishes whether or not the claimed identity has one or more of the following properties:

- **Existence/liveness:** It exists at the time of enrollment (i.e., the person is alive and present) and can be localized (i.e., the person can be reached through their address, phone number, or email).
- **Uniqueness:** It is claimed by only one individual (i.e., the person is unique in the database). This process is also called de-duplication and can be accomplished using combinations of a variety of attributes (although biometrics are currently the most accurate).²¹
- **Linkages:** It can be linked to existing social identities, such as those in existing identity databases, civil registries, population registries, tax registries, property registries, social security databases, police records, etc.²²

BOX 2

Establishing a Minimum Set of Unique Identity Attributes

A **minimum set of unique identity attributes** is the set of data attributes that uniquely represents an individual, and is usually available from a national identity system. It is essential for establishing digital identity across actors within a country's ecosystem and also across borders. It typically contains a number of mandatory attributes but may also contain one or more additional optional attributes. For example, the European Union's eIDAS Implementing Regulation (2015/1501) established that the minimum data set of unique identity attributes for a natural (i.e. a physical) person includes both *mandatory attributes* (current family name(s), current first name(s), date of birth, and a unique identifier which is as persistent as possible in time) and *additional attributes* (first and family name(s) at birth, place of birth, current address, gender).²³

It is the responsibility of the state to ensure that when establishing a legal identity, a minimum set of attributes uniquely representing the individual in question is provided, in accordance with the technical specifications, standards, and procedures set forth in the law. Furthermore, it is recommended that private sector entities follow the same principle when creating user identities for online authentication so that third parties are able to confirm an individual's digital identity with an appropriate degree of confidence. However, according to best practices, authentication for an online service should require only those attributes that are adequate, relevant, and not excessive to grant access to the service. Using attributes disproportional to the use case puts user data and privacy at risk.

Issuance

A registered identity goes through an issuance or credentialing process before it can be asserted (i.e.,

used) by a person. Traditionally, ID issuers provided documents (e.g., a birth certificate) or credentials (e.g., eDocuments, (e)IDs, (e)Passports). For an ID to be considered digital, the credentials or certificates

21. Gelb and Clark, 2013.

22. World Bank, 2014.

23. For more information, see <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1501>

issued must be electronic, in the sense that they store and communicate data electronically. Types of electronic credentials include

- **Smartcards:** These cards offer advanced security features and record digital credentials and/or biometric data on an embedded computer chip. Smartcards can come in the form of a contact/contactless card, or Near Field Communication (NFC)-enabled SIM card. Data stored on a smartcard can be accessed offline for authentication where there is no internet connection or mobile network.
- **2D Bar code card:** Cards can be personalized with an encrypted 2D bar code containing a person's personal data and biometrics, either instead of or in addition to a chip. The 2D bar code is a secure and cost-efficient mean to provide a digital identity and to authenticate holders using biometrics. It has been widely deployed in Africa, Latin America, and the Middle East, including Lebanon, Mali, and Ghana, and more recently in Egypt to authenticate holders during the last elections.
- **Mobile identity:** Mobile phones and other devices can be used to provide portable digital identity and authentication for a variety of online transactions. For example, providers can issue SIM cards with digital certificates or use other mobile network assets that can enable secure and convenient identity and authentication of users for eGovernment (eGov) services and other public or private platforms.
- **ID in the cloud:** Unlike portable credentials such as smartcards and SIM cards, some systems store certificates and biometrics on a server only. In this case, a physical credential may not be issued, or may be issued in non-electronic form (e.g., India's Aadhaar program issues only a paper receipt). A tamper-resistant environment for secure cryptographic key generation and management will increase the security of an ID in the cloud against theft.

Authentication

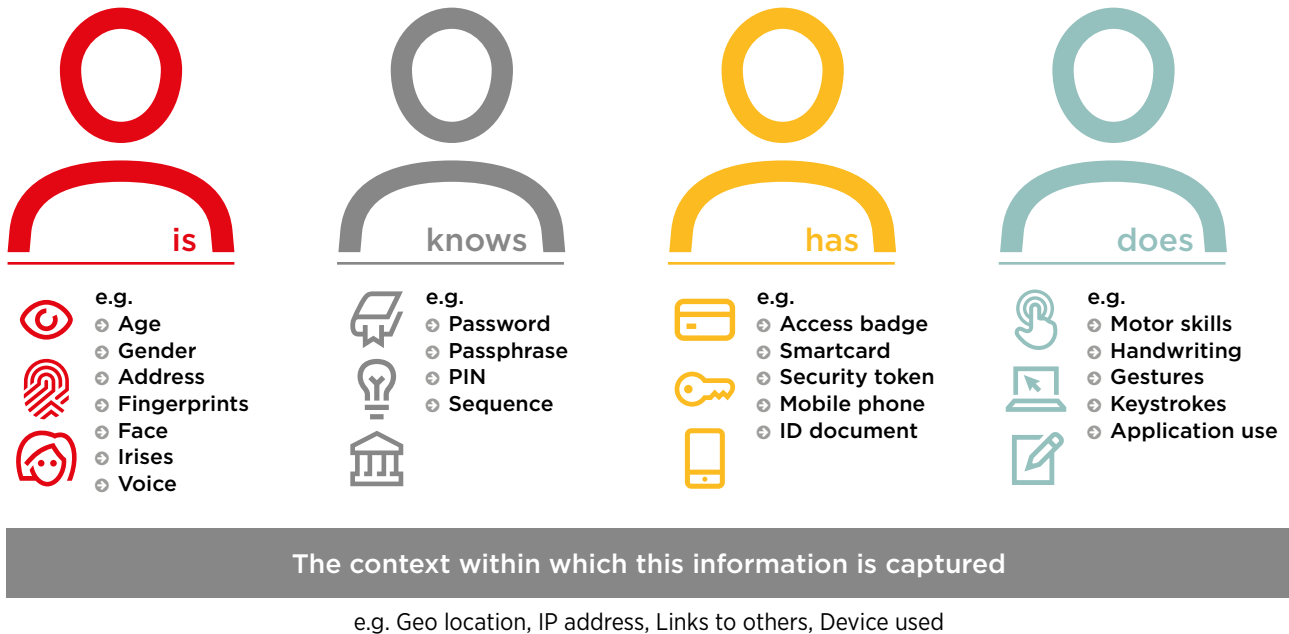
Once a person has been registered and credentialed, they can use their digital identity to access the associated benefits and services. For example, citizens may use their eID number to pay taxes through an eGov portal, while bank customers can use smart debit cards or mobile financial services to make purchases. In order to access services, the user must be authenticated using one or more factors that generally fall into one of four categories illustrated in Figure 2: what a person is, what she knows, what she has, and what she does. Authentication using these attributes can occur through various pathways, including

- **Smartcards:** People with smartcards can authenticate their identity using multiple authentication factors for varying levels of assurance. For example, a simple PIN for low risk use cases or a digital signature based on public key infrastructure (PKI) technology for high risk use cases. Fingerprints can be used to establish a non-ambiguous link with the user. Because they store data locally on a chip, smartcards can also be used for offline digital authentication or remote locations where connectivity is limited.
- **Mobile identity:** Using smartphone applications, USSD or SMS-based authenticators, or SIM cards, mobile identity can incorporate multiple authentication factors for varying levels of assurance. For example, a simple PIN for low risk use cases, multiple-factor authentication solutions (including with the use of biometrics) or a mobile signature based on public key infrastructure (PKI) technology with a secure element (SE) for high-risk use cases. Authentication can be strengthened by using third and fourth factors such as the individual's location or behavior.
- **ID in the cloud:** Instead of issuing an identity document or mobile credential, a digital identity system can rely on biometrics for remote authentication. In this case, an identity is asserted and verified via a computer or other device with a biometric reader that connects to the cloud. A cloud-based system eliminates the need and cost of physical credentials, but requires robust ICT infrastructure for connectivity.

FIGURE 2 Source: Authors' analysis, based on World Bank, 2015a.

Common Authentication Factors

WHAT A PERSON...



Lifecycle Management

Throughout the lifecycle, digital identity providers manage and organize the identity system, including facilities and staff, record keeping, compliance and auditing, and updating the status and content of digital identities. For example, users may need to **update** various identity attributes, such as address, marital status, profession, etc. In addition, identity providers may need to **revoke** an identity, which involves invalidating the digital identity for either fraud or security reasons, or **terminate** an identity in the case of the individual's death.

Levels of Assurance

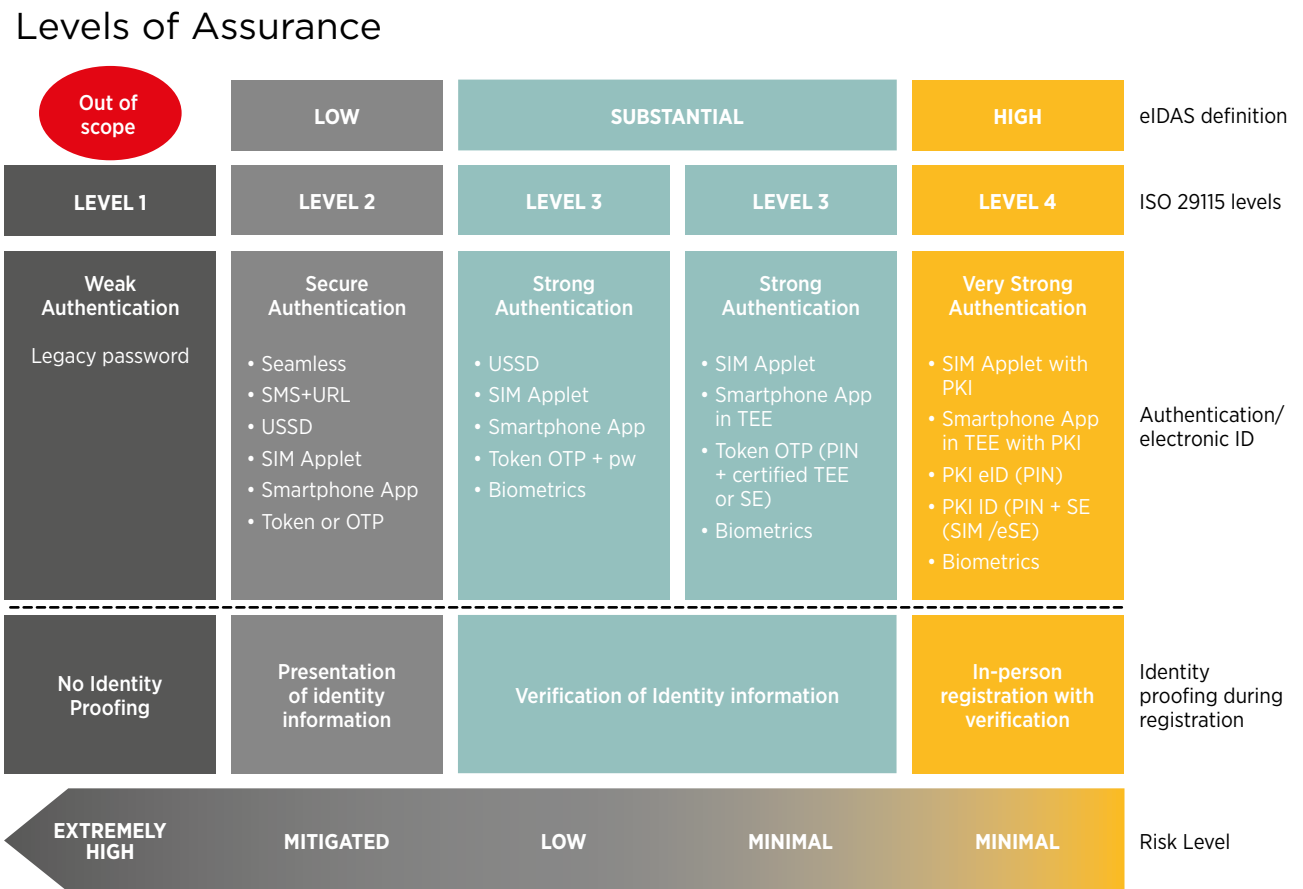
When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that she is who she claims to be depends

on the degree of security assurance provided and the context in which the information is captured, referred to as the **level of assurance (LOA)**.²⁴ Assurance levels depend on the strength of the identification and authentication processes, and are critical to access control and reducing identity theft. As depicted in Figure 3, the higher the LOA, the lower is the risk that service providers will rely on a compromised credential during a transaction. For "identity proofing", the LOA is dependent on the method of identification, including the scope of personal information and attributes collected about an individual during enrollment, and the degree of certainty with which these attributes are ascertained (i.e., whether or not they are validated). For example, if personal data are collected during enrollment but not de-duplicated or checked against existing databases for veracity, this would constitute a low LOA because there is no validation of the identity information.

24. Examples of existing standards for security assurance level for digital identity and authentication include: ISO29115/IEC DIS; UK Cabinet Office; European Commission, etc. There are four Levels of Assurance (LOA) in accordance with ISO 29115:

1. LoA1 - no identity proofing; little confidence that this is the same person
2. LoA2 - basic identity proofing; single factor of authentication (e.g., username/password or possession and control of a device)
3. LoA3 - more stringent identity proofing; multi-factor authentication [e.g., something I have (the device) + something I know (a PIN)]
4. LoA4 - in-person identity proofing required; strong cryptographic authentication of all communicating parties and all sensitive data transfers between the parties (e.g., mobile signature)

FIGURE 3 Source: Author's elaboration.



Key: OTP = one-time password; PKI = public key infrastructure; (e)SE = secure element or embedded secure element (a tamper-resistant hardware platform); TEE = trusted execution environment (a secure area of the smartphone); USSD = unstructured supplementary service data (“quick codes”). Note: NISTIC 800-63A draft standard guidelines on identity proofing also allow for virtual-in person proofing and enrollment transactions²⁵

For authentication, the strength of the identity credential and authentication depends on the robustness of the technology and the authenticators used. Different types of transactions will require different LOAs, and not all transactions will require the highest level—the greater the risk of the transaction, the greater the assurance level must be. Typically, single factor authentication—such as ID number or knowledge of a password—is not sufficient to prove a person’s identity or provide accurate authentication. This level of risk may be appropriate for some

applications (e.g., checking Facebook) but higher security transactions (e.g., collecting benefits or signing an official document) may require additional or multiple factors of authentication to augment the user’s credentials. These factors must be robust and secure.²⁶ The possession of a secure device, such as a physical token, a mobile phone, or a smartcard allows for secure authentication and can be complemented by a personal identification number (PIN) or attribute (such as a biometric feature or behavior) in order to provide stronger security.²⁷

25. Source: <https://pages.nist.gov/800-63-3/sp800-63a.html> and <http://nctic.blogs.govdelivery.com/2016/05/08/announcing-draft-special-publication-800-63-3-digital-authentication-guideline/>

26. The robustness and security of these factors comprises three elements:

1. Authentication robustness - Is this the same person?
2. Security robustness - Is the authentication tamper-proof?
3. Identity proofing robustness - Who is this person? How much do I trust the veracity of the information provided?

27. One example of an authentication protocol is GSMA’s Mobile Connect solution, which enables customers to create and manage a digital universal identity via a single login. The solution works by employing the user’s unique mobile number combined with a unique PIN and secure network of the mobile operators to ensure the validity of the mobile device and user for more secure use cases, including government services. It enables the use of mobile operator data and business process to enhance user security and combat identity theft.

Stakeholders and Roles

Within any identity ecosystem, there are a number of primary stakeholders that play varying roles in the identification and authentication processes depending on the country context and the type and scope of the digital identity (e.g. a national eID vs. an online banking platform). In general, individuals (e.g., citizens or clients) are the primary end-users in a system, while government bodies and private firms are the primary providers of digital identity, authentication, and services. Other key stakeholders are public actors responsible for regulation, and public and private actors responsible for standard setting and trust building. A summary of main stakeholders and the typical roles they play in the digital identity ecosystem is provided in Table 1 below; Figure 1 above illustrates where these roles fall within the identity lifecycle.

End-Users

- **Individuals:** Individual citizens and clients are the end-users of digital identity systems. They enroll in identity systems and use the credentials they receive to access the benefits and services of a given country or company.

Providers

- **Government bodies:**
 - **Legal registrars** are the agencies in charge of providing legal identification to citizens. This may include national identification authorities (NIAs) in charge of creating and maintaining national ID cards and other documents, as well as national population registers and birth registers that record life events.
 - **Functional registrars** are agencies that create and maintain identity registries for a specific purpose or service, including electoral commissions, tax agencies, social security authorities, hospitals, etc. These registries may be linked to legal registries such as a national population register, or they may be separate identity systems.
 - **eGov service providers** are government agencies or platforms that provide online services to

citizens or residents which require some proof of identity and entitlements. Oftentimes, they are linked to the national identity system and/or functional registers. Examples include EESTI (Estonia), MyGov (Australia), Gov.UK Verify (UK), Hukoomi (Qatar), Suomi (Finland), eAlbania, etc.

- **Private firms:**
 - **Commercial service providers** are firms that either use digital identities in order to provide services to their clients and/or enable end-users to transact in a digital environment providing digital identity and authentication services. This includes banks, mobile network operators, utilities, healthcare providers, online commerce platforms, credit rating agencies, etc.
 - **Identity solution suppliers** are firms that provide hardware, software, and support for the development of digital identity systems. They may be contracted to provide a specific set of inputs at a particular stage in the digital identity lifecycle, or may provide services on an ongoing basis.

Government bodies generally play one or more principle roles in the digital identity lifecycle, at times in partnership with the private sector:

- **Digital identity providers** are those actors that create digital identities for users by registering them (including enrollment and validation) and issuing documentation or credentials. In general, identity providers also store and manage data and credentials on behalf of the users. In the public sector, legal registers are the most common digital ID providers, although functional registers, such as electoral commissions may also create and manage digital identities (e.g., a voter register). Commercial service providers are also frequently digital identity providers. For example, mobile companies provide SIM cards and banks issue debit cards, in each case after enrolling and verifying the identities of their customers. Oftentimes, private identity providers rely upon or use legal identity provided by the public sector (e.g., your SIM card may be linked to a national identity number).

- **Attribute providers** are entities that hold verified user data and either verify or provide these attributes to third parties (subject to user consent). Such information may pertain to the individual's identity data (e.g., name, address, age, gender, etc.), or data related to the credential device (e.g., network information data about the individual) or any other information about the user including other linked identifiers such as telephone number, email address, national insurance number, social security number student enrollment number, etc. In many cases, there is overlap between digital identity and attribute providers. In some cases, however, actors provide attributes upon request of the identity providers or relying parties.
- **Digital authentication providers** verify a user's attributes or identity in order to determine his or her right to access a service or benefit. In the public sector, those agencies that are directly involved in delivering services that require verification—including functional registers and eGov service providers—are commonly authentication providers. In some cases (e.g., Aadhaar), national ID authorities will also authenticate on behalf of a service provider. In the private sector, commercial service providers authenticate users.
- **Service providers** are those entities that provide services directly to end-users (citizens and clients). This may include public agencies such as functional registrars and eGov service providers, as well as private service providers. Service providers may themselves be digital ID and authentication providers, or they may outsource these functions to other agencies.

Enabling and Supporting Actors

The work of digital identity, authentication and service providers is embedded in the larger ecosystem of public and private actors who enable and support identity systems, including:

- **Regulatory and oversight agencies** and organizations regulate, control and audit digital identity systems. This includes primarily national-level public sector agencies, and supra-national

authorities such as the European Data Protection board, EU MSs Supervisors as per eIDAS requirements. In addition, there are a few instances of self-regulatory bodies like T-Scheme in the UK.²⁸ The goal of these actors is to ensure that digital identity and authentication providers follow legal standards and best practices for the collection, storage, and use of personal data.

- **Standard setting bodies** are organizations that provide protocols for digital identification and authentication. This includes public sector agencies such as European Committee for Standardization (CEN), and NIST, as well as private and non-profit organizations such as the ISO standard body, the Open ID Foundation, FIDO Alliance, GSMA, and Secure Identity Alliance. The goal of these agencies is to increase interoperability and build open and scalable identity solutions.
- **Identity organizations and trust frameworks** define technical, operational, legal, and enforcement mechanisms for information exchange related to identity management. This includes public sector actors such as the Trust Framework Provider Adoption Process (TFPAP) developed by the U.S. Identity, Credential, and Access Management (ICAM) subcommittee in partnership with the non-profit Open Identity Exchange (OIX), and private sector actors like the Mobile Network Operators developed solution Mobile Connect.
- **Donor agencies and development partners** including the World Bank and regional development banks, the European Union, IOM, IMCPD, UNHCR, UNDP, UNICEF, USAID, the Gates Foundation and others provide support in the form of funding and technical assistance for the development of digital identity systems. In some cases, this support may be intended to generally strengthen the country's identity system, and in other cases it may be one component of a program that requires identification (e.g., electoral support, cash transfer programs, etc.). In the latter case, donors may also be providers of identity, authentication, and services (e.g., UNHCR uses a biometric registry to distribute food aid to refugees).

28. T-scheme is the independent, industry-led self-regulatory scheme set up to create assessment criteria against which it will approve Trust Services <http://tscheme.org/about/>

TABLE 1

Key Identity Stakeholders and Roles

	STAKEHOLDERS	ROLE	PRIMARY GOALS
END-USERS	Individuals Voters, migrants, bank customers, etc.	<ul style="list-style-type: none"> End users 	<ul style="list-style-type: none"> Accessibility User-friendliness Data protection & privacy
GOVERNMENT PROVIDERS	Legal registrars National ID agency, e.g., UIDAI (India), NADRA (Pakistan); national population or birth register, passport agency, etc.	<ul style="list-style-type: none"> Digital ID providers Attribute providers Authentication providers Service providers 	<ul style="list-style-type: none"> Effective & efficient services Security & user trust Fraud reduction Universal coverage & access
	Functional registrars Electoral commission, tax agency, social security authority, pension office, hospitals, etc.	<ul style="list-style-type: none"> Digital ID providers Attribute providers Authentication providers Service providers 	<ul style="list-style-type: none"> Effective & efficient services Security & user trust Fraud reduction Universal coverage & access
	eGov service providers Gov.UK Verify (UK), EESTI (Estonia), EIDO (UAE), HUKOONI (Qatar), etc.	<ul style="list-style-type: none"> Authentication providers Service providers 	<ul style="list-style-type: none"> Effective & efficient services Security & user trust Fraud reduction
PRIVATE PROVIDERS	Private firms Mobile network operators, banks, utilities, healthcare providers, online commerce platforms, credit rating agencies, hardware and software developers, systems integrators, total solution providers, etc.	<ul style="list-style-type: none"> Digital ID providers Attribute providers Authentication providers Service providers Identity solutions suppliers 	<ul style="list-style-type: none"> Effective & efficient services Security & user trust Fraud reduction
ENABLING AND SUPPORTING ACTORS	Regulatory agencies <i>Public sector:</i> National agencies; supra-national authorities (European Data Protection Board, EU MSs Supervisors as per eIDAS requirements or self-regulatory bodies like T-Scheme in the UK).	<ul style="list-style-type: none"> Regulation & oversight 	<ul style="list-style-type: none"> Consistent identity management Data protection & privacy Security & user trust
	Standard setting bodies <i>Public sector:</i> CEN, NIST. <i>Private & non-profit sector:</i> ISO standard body, IEEE, Open ID Foundation, FIDO Alliance, GSMA, Secure Identity Alliance, ETSI, Biometrics Institute, 3GPP, OMA, etc.	<ul style="list-style-type: none"> Standard setting 	<ul style="list-style-type: none"> Build open, scalable, interoperable, and robust identity solutions
	Identity organizations & trust frameworks <i>Public sector:</i> TFPAP, USGSA. <i>Private sector:</i> Mobile Identity (Finland), digital identity banking federation (Scandinavia), and Mobile Connect, etc.	<ul style="list-style-type: none"> Trust building 	<ul style="list-style-type: none"> Establish trust among digital identity ecosystem stakeholders
	Donor agencies & development partners World Bank, European Union, IOM, IMCPD, UNHCR, UNDP, UNICEF, USAID, Gates Foundation, etc.	<ul style="list-style-type: none"> Funding & Technical assistance Digital ID, authentication & service providers 	<ul style="list-style-type: none"> Support client government goals Effective & efficient donor program delivery Capacity building

Digital Identity Ecosystems: Existing Landscape of Public and Private involvement

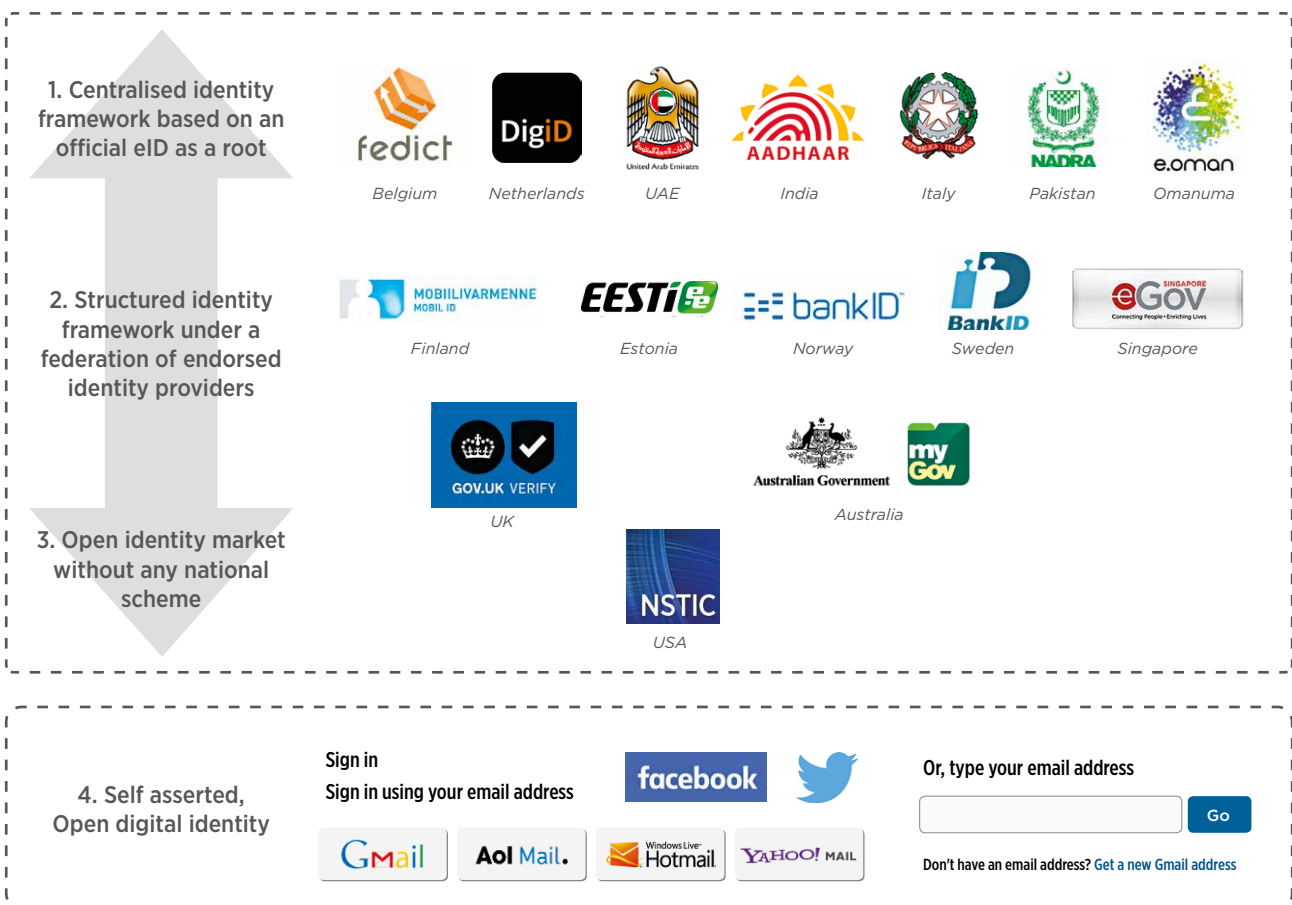
Governments and private sector firms share a common interest in promoting robust digital identity systems that enable identification and authentication of end-users for a variety of functions and services. Furthermore, both public and private stakeholders may rely on each other to build and manage identity systems. For example, governments may outsource various aspects of their identity architecture to private firms (e.g., system development), and may also collaborate with the private sector to ensure interoperability of an official ID with private services (e.g., for metro passes, KYC requirements, etc.).

Similarly, private firms often rely on official forms of identification (e.g., birth certificates, national IDs) to validate the identity of their users.

We see increased potential for public-private collaboration in building digital identity ecosystems. This section takes stock of the current types of ecosystems that countries have developed to provide digital identity services for public and private use, and offers key considerations for partnerships to build more advanced digital infrastructure.

FIGURE 4 Source: Author's elaboration.

Examples of Digital Identity Ecosystems



Ecosystem Types

At present, digital identity ecosystems at the national level can be loosely categorized into four types that result from different cultural, legal, and political approaches to identity management. These types vary based on the degree to which core digital identities—those used as the basis for most public and private transactions and for identity verification by secondary identity providers—are centralized or decentralized and whether or not they are provided by the public or private sector. As illustrated in Figure 4, they can be thought of as a continuum, with significant variation between countries:

1. The first type of ecosystem is a **government-driven centralized system** where individuals' identity attributes are stored in one or more government-owned database(s) and state-issued eID serves as the basis for all or most digital transactions for both the public and private sectors (e.g., Belgium, Germany, UAE, Italy, Pakistan, Malaysia). Furthermore, the official eID can be used as the basis for verifying other digital identities, such as banking and mobile phone credentials.
2. The second is a **semi-centralized, federated system** of multiple, government-endorsed digital identity providers (e.g., Sweden, Finland, UK, Australia). In a semi-centralized system, citizens are free to choose between multiple trusted identity providers (e.g., banks, mobile operators, etc.) and use these credentials to access a broad range of public and private digital services via an identity hub or gateway that facilitates authentication across multiple platforms. In this type of ecosystem, private firms often play a key role as digital identity providers, after governments offer an official basis of identification using breeder documents (such as birth certificates). However, public agencies may also be trusted identity providers, and the government plays a central role in defining and regulating the identity framework and endorsing providers.
3. Third is a **decentralized, open Identity market** without any national scheme (e.g., USA). In a decentralized, open identity system, public and private sector organizations create, utilize and manage their own digital identities on the basis of a self-regulated framework. In the USA for example the a National Strategy for Trust Identities in Cyberspace (NSTIC) has taken steps to create a user-centric "Identity Ecosystem" of public and private sector organizations that utilize secure, efficient, and interoperable identity solutions to access online services in manner that promote confidence, privacy, choice and innovation. The strategy is completely voluntary and focused on providing high level guidance to the private sector.²⁹ This model not yet been utilized in a developing country context in the absence of credible national identification and low birth registration rates.
4. The fourth type is a **self-asserted digital identity** ecosystem driven by the largest internet players (e.g., Facebook, Google, Yahoo and other internet platforms). In a self-asserted ecosystem, users choose their own digital identity attributes, and no verification against official identity documents is required, resulting in a lower level of security. At the time of writing there are no examples of countries that have considered this approach to provide access to their digital services, and it is thus out of scope for this paper.

Considerations for Strengthening Identity Ecosystems

While governments will nearly always play a large role in digital identity systems, the scope and mode of private sector participation will depend on the particular context, needs, and financing constraints. When choosing an appropriate model for digital identity infrastructure and services, stakeholders should consider the existing identity landscape, the capacity of government systems, and the ability of the private sector to provide the required level of security and privacy protection.

29. In addition, the government has also funded the start of a private sector led Steering Group - the Identity Ecosystem System Steering Group (www.idesg.org). The IDESG includes representatives from over 200 organizations, that just recently released the Identity Ecosystem Framework to provide a baseline set of standards and policies for private and public organizations to follow. The Framework can be found here: <http://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents>. They are about to roll out a Listing Service for companies to self-certify that they meet some or all of the framework. <http://www.idesg.org/The-ID-Ecosystem/Registry>

Identity Landscape and Government Capacity

The landscape of identification that already exists in the country will shape the development of digital identity ecosystems and the nature of private sector participation. Countries vary substantially in their existing identity architecture and capacity, including the extent to which government agencies maintain centralized records of a majority of the population and whether these records are digitized. In many low-income countries, identification is local and offline, or “village-based”, and the overall volume of identity-based transactions is low. In these cases, the private sector may offer some infrastructure for online transactions (e.g., mobile-based), but this will be limited by the lack of robust official identification as a source of trusted identity. Countries with more developed administrative capacity generally have centralized identity management systems that are increasingly digital, which allows for a rapid increase in the volume of id-related transactions for both public and private service providers.

The strategy for digitizing identity systems depends on a number of issues, including a country’s approach to privacy and security and existing legacy systems and identity management models. Common to all models is the need to create secure, reliable, and trustworthy digital identity credentials. This requires the existence—or creation—of robust databases that underpin the issuance of secure credentials which can be used as a foundation for both public and private sector identification and authentication.³⁰ For example, in countries with digitalized civil identity or population registers:

- Private sector companies may use a minimum set of unique identity attributes from the government identity provider in order to issue their own user credentials. Then, these private sector-issued credentials or tokens can be used for identification, authentication, and authorization purposes. Private sector organizations assert the identity of the user and act as digital identity and authentication providers (e.g., Finland’s semi-centralized system or Estonia centralized system).

- In other countries there is potential for trusted private sector entities to provide electronic identification and authentication for government and private services using verified private sector complementary attributes under a semi-centralized certified scheme (e.g., the United Kingdom).

Even if a unique database exists, however, it commonly does not contain all of the attributes required to provide a specific service. In this case, an identity model might consist of a combination of unique identification provided by the state and complementary attributes collected by the private sector (See Box 2 for the example of the EU, Aadhaar and Estonia are others). In order to ensure interoperability between systems (both public and private), stakeholders must come to a consensus on a minimum set of identity attributes.

In countries with inadequate or nonexistent civil registration or national identity systems, there may be a role for private sector actors to play in supporting the government in the creation of an official digital identity that can be authenticated and used for a variety of online and analogue services. See for example the role of corporate social initiatives undertaken by the mobile operators in Ghana, Tanzania, Pakistan, Senegal and Uganda for birth registration purposes.³¹

In all circumstances, the roles and responsibilities of both public and private sector organizations must be clearly defined ahead of time to ensure transparency, and the definition of what constitutes official legal identity should remain the purview of governments and their citizens.

Privacy and Security

Another critical issue is the capacity of the private sector to provide trustworthy digital identity, offering the same standards of privacy and security protection as those provided by the state, for similar services and in compliance with national privacy regulations (along with international conventions, where applicable, national sovereignty and governance principles). For example, there is a difference between those companies that are

30. See Alan Gelb, 2016, p. 4.

31. See, for example, Uganda Mobile Vital Records System is using mobile technology to overcome the poor communication network between rural villages and registration offices. Thanks to mobile phones, village registration agents are able to record births and send details about vital events on new-borns for legal registration. The data is transmitted to local hospitals via a 3G web-based application and then is stored in a computer database. A challenge will be how to tying the data to the identity of the child as it matures and progresses through society, school, work, migrates, etc., including ensuring continuity of identity and choice and control as the child becomes mature enough to exercise legal rights.

bound by national legislation and privacy frameworks and companies that operate globally but are not obligated to adhere to local privacy laws.

Benefits of public-private cooperation

There are a number of benefits to public-private cooperation to build digital ID ecosystems, including:

- **For Governments:** Digital transformation, modernization and use of integrated systems will reduce cost of implementation and interoperability by allowing for the secure transfer of citizen data and lowering existing barriers to entry for governments to harmonize national digital identity systems. Private sector companies may be positioned to leverage existing assets and footprint, helping to drive efficiency and scale in the development of digital identity ecosystems.
- **For the private sector:** Enlarging the digital identity ecosystem and enabling private sector parties to create a trusted identity ecosystem between the government and the private sector itself. A stronger

government identification system will increase the private sector's ability to offer services that are useful and valuable to consumers, enabling more efficiency in service delivery. Building trust between eco-system partners can help accelerate innovation and stimulate investment.

Managing Risks

However, while a public-private partnership can offer benefits to the development of a digital identity program, cooperation also comes with risks that need to be outlined and managed by both the government and the private sector. Adequate risk mitigation by the government is required to ensure that the digital identity program (whether for legal or functional use) is based on good governance, open standards, fiscal efficiency, user affordability, and operational effectiveness, and promotes innovation and a competitive marketplace. Similar measures are required by the private sector to ensure that contractual agreements are upheld, financial investments are protected, and a level playing field is available for market players.

Models for Private Participation in Official Digital Id Systems

In addition to public-private cooperation to develop digital identity ecosystems more broadly, we have begun to see a range of partnerships that focus specifically on strengthening government identity systems. In European countries such as Estonia, Finland, Norway, Switzerland, and the United Kingdom, for example, the private sector—and the mobile industry in particular—has played a key role in building national digital identity systems and authentication programs and unlocking the potential of digital identity for the economy through leveraging existing assets and business processes.³² We have now begun to see similar partnerships in developing countries that have sought to extend the

coverage of their identity systems by utilizing private sector cooperation, services, and investment.

When it comes to public-private cooperation for the provision of national digital identity systems, models vary based on the type of the project and the scope of private sector involvement, as shown in Figure 5. Traditionally, the most common form of private sector participation in national identity systems has been as suppliers of publicly procured inputs—including hardware, software, systems design, etc.—used to build a national identity database and/or to set up identity authentication and verification³³ (e.g., Pakistan and

32. For example, see GSMA case studies such as: *Finnish Mobile ID: A Lesson in Interoperability*; *Estonia's Mobile-ID: Driving Today's e-Services Economy*; *Norwegian Mobile Bank ID: Reaching Scale through Collaboration*; *Swisscom Mobile ID: Enabling an Ecosystem for Secure Mobile Authentication*; *Mobile Signature in Turkey - A Case Study of Turkcell: MobilImza*; *Mobile Birth Registration in Sub-Saharan Africa: A case study of Orange Senegal and Uganda Telecom solutions*.

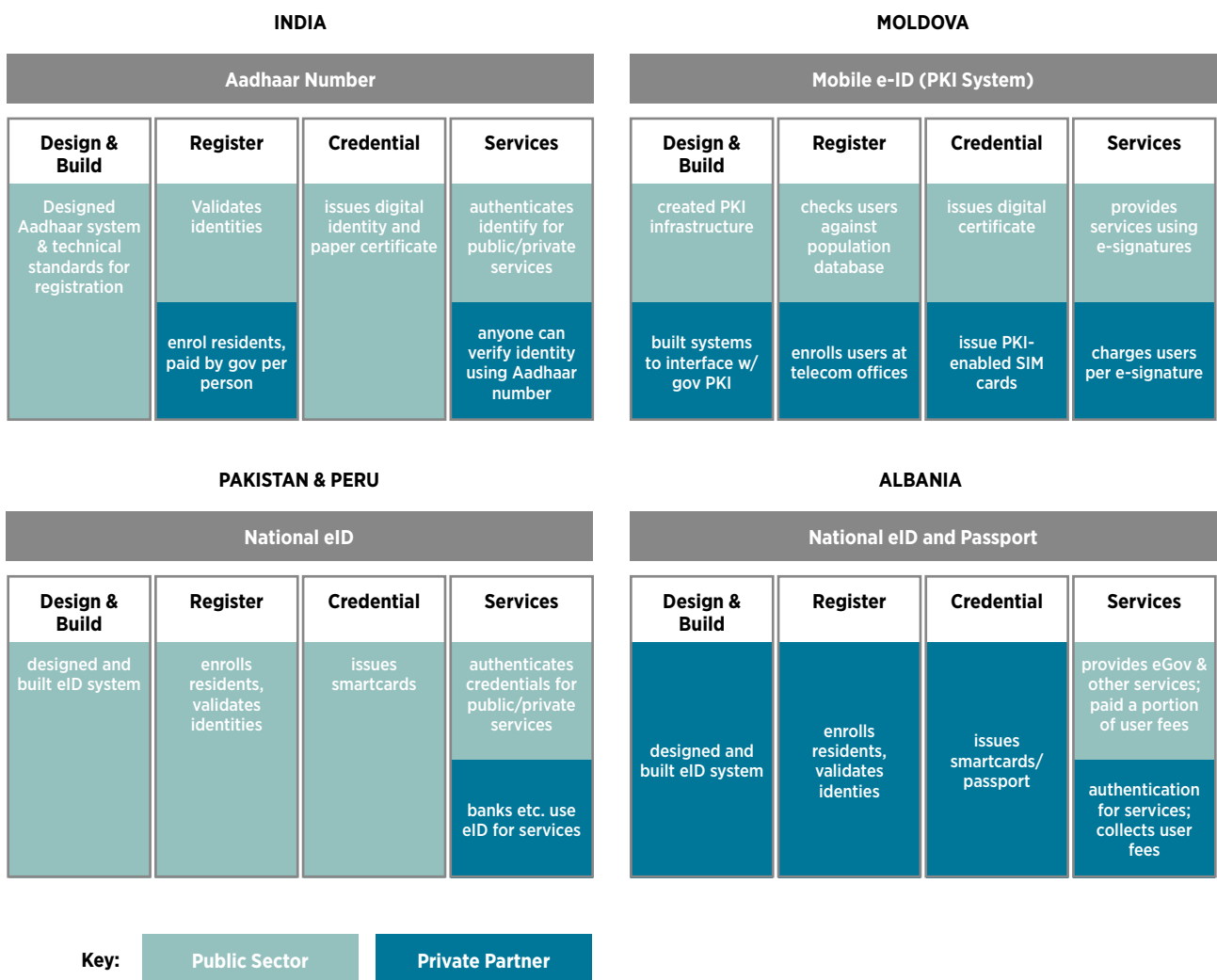
33. In the latter case, the private contractor leverages the value of the digital identity system and may introduce a fee system based on authentication requests from private companies (e.g. mobile, credit rating agencies, smart card providers, etc.) or the public sector. In the UK, for example, the Identity Assurance Programme (IDAP) took a procurement approach for their government certification program, which enables private sector organizations—including mobile network operators and other private providers—to become authorized digital identity providers. A Draft of Identity Assurance Provider Framework Agreement is available here (<https://data.gov.uk/data/contracts-finder-archive/contract/1690273/>) which also include a description of the charges structure used in the agreement between the government and the identity assurance private sector providers. See Accenture study, forthcoming for more examples.

Peru). In some countries, governments have begun to consider Public Private Partnerships (PPP) such as BOTs (build-own-transfer) or concessions (e.g., Albania), service agreements (e.g., India, Nigeria, Moldova), and other arrangements that specify a deeper level of private sector engagement. In order to highlight the

emerging ways in which the private sector is involved in the provision of national digital identity, the remainder of this section focuses on private involvement that goes beyond traditional procurement-type contracts (which are plentiful and generally well known).³⁴

FIGURE 5 Source: Author's elaboration

Examples of Private Sector Involvement in Official Digital Identity Systems



Note: Figure depicts who is responsible for the primary activities in each phase of building an official identification system. In reality, even phases for which one sector has clear responsibility often involve a supporting role for other actors. For example, although the government executed the design and building phase in the cases of India, Pakistan, and Peru, the private sector was involved as a supplier of key hardware and/or software inputs. Similarly, even though Albania awarded a complete concession to a private company, the government was still involved in planning and oversight.

34. In a typical public procurement project, governments contract vendors to supply a defined set of inputs or outputs, funding capital expenditures and retaining ownership of assets (and risk). In this model, the national or regional government is responsible for the set-up and delivery cost of the technology solution and bears the responsibility of its running costs, although they may look to the private sector to bring in needed expertise and efficiencies.

Partnerships for Digital Identity

We surveyed a number of cases of significant private-sector involvement in national digital ID systems, including Albania, Chile, Estonia, Finland, India, Moldova, and Nigeria. These cases are not exhaustive,³⁵ but illustrate a variety of potential models. In general, they can be placed in categories along two dimensions. The first is the **type of partnership**, either a service agreement or a BOT/concession, while the second is the **scope of partnership**, whether it covers registration of digital IDs or the provision of services. Within these categories, there is variation in the degree to which private firms are involved in (1) **designing and building** identity infrastructure, (2) **financing** initial and ongoing capital investments, and (3) **operating and maintaining** digital identities throughout their lifecycle, including registration, issuance, authentication, and services. There is also variation in whether the **source of revenue** for private firms is government fees or user fees. See the Annex for more case details.

Although these examples are illustrative of different models of partnerships, it is important to highlight the fact that not all models will be appropriate in all countries. For example, the context—including political, institutional and technological maturity—of identification systems in countries such as Estonia, Finland, and Albania is quite different from that of many countries in Africa, Asia, and Latin America.

Service Agreements

In the service agreement model, the government contracts with a private firm or firms to undertake a specific role in one or more stage of the digital identity lifecycle. In these cases firms receive revenue directly from users, or from the government on a performance basis. Whether or not these agreements meet the strict definition of a PPP above depends on the extent to which they are long-term partnerships (most are) that require significant investment on the part of the private actor.³⁶ Key examples include:

- **India:** The Aadhaar program relies on private firms to enroll residents' biographic data and biometrics, which are then sent to India's Unique Identification Authority (UIDAI) for validation and issuance. UIDAI enters into MOUs with public and private Registrars (e.g., banks and insurance agencies), who contract with other firms as Enrollment Agencies that meet UIDAI's rigorous technical standards. Enrolling agents are then paid by the government on a per-transaction basis.³⁷
- **Nigeria:** Nigeria's Identity Management Commission (NIMC) has begun to issue new smartcards in partnership with financial service companies. These cards are linked to a pre-paid account number with a participating bank that can be used by the cardholder for public or commercial transactions at accepting merchants. The cards are intended to create demand for connectivity and electronic services in Nigeria.
- **Estonia, Finland, & Moldova:** Each of these countries has partnered with mobile network operators to deliver mobile authentication services to eID cardholders. In each case, the mobile companies issue users with a PKI-enabled SIM, and then charge a per-use fee when they use a digital signature to authenticate themselves for eGov and other online services.

BOT/Concessions

In contrast to service agreements, where the government contracts limited (though potentially vital) aspects of a project to private firms, build-own-transfer (BOT) or concession-type partnerships are ones in which the private sector is solely or primarily in charge of designing, building and operating a project, usually for a fixed concession period. These are considered PPPs according to standard definitions, as the contracts bundle together many services and entail significant risk and financing on the part of the private party. In these cases, contracts are often awarded to a single

35. Pakistan's ID system involves a different type of private sector involvement. Its National Database and Registration Authority (NADRA) is an autonomy agency that contracts with the Pakistani government to provide identity services. NADRA also delivers identification and system integration solutions internationally, and its clients include the governments of Sudan, Kenya, Bangladesh, Sri Lanka and Nigeria.

36. For a categorization of PPP arrangements in eGovernment systems, see World Bank, 2015b. The Bank's PPP Knowledge Lab (<https://pppknowledgelab.org/>) is also an excellent resource for understanding PPPs for infrastructure development and defines a PPP as a "long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance."

37. UTI, 2014.

contractor or consortium, project costs and outputs are predetermined, and payment is performance-based and can include a fixed set up cost. Revenue generated by the ID system is allocated between the private and public sectors according to the contract.

Key examples include:

- **Chile:** Chile's Registro *Civil e Identificación (SRCeI)* awarded a concession to a private firm to modernize its existing civil identification system through building, installing, and maintaining new hardware and software, integrating databases, training SRCeI staff, and personalizing eID smartcards and passports. The government operates the system and pays a fee per document issued.
- **Albania:** Uniquely, Albania's Ministry of Interior Affairs has awarded a full concession to design, build, operate, and maintain an eID and e-passport system. The firm is in charge of enrolling residents, issuing IDs, and collecting usage fees, a portion of which are paid back to the government. In 2013, the original concession was extended for an additional 10 years.

Scope of Partnership

In addition to the distinction between service agreements and BOT or concession-based partnerships, we can categorize these partnerships according to stage in the lifecycle in which the private sector is involved:

- **Registration:** A few of the cases have involved public actors undertaking all or part of the effort to register citizens in the creation of a new national digital identity system. Logically, this includes the BOT/concession type partnerships where firms are involved in designing, building, and operating the ID system for a fixed period of time (e.g., Chile and Albania), but may also include service agreements (e.g., India).

- **Services:** A majority of the digital identity cases with public-private cooperation involve the provision of services to end-users, after enrollment has been conducted by the public sector. This is expected given that private sector service providers are primary stakeholders in the creation of digital identity. Many service-based partnerships have been added on to already existing digital ID systems (e.g., Moldova, Finland, and Estonia). An exception to this is Nigeria, where the smartcard service agreement was designed into the project from its onset.

Choosing a model

Each country context is unique, and a thorough analysis of this context is necessary before adopting a particular business model. The selection of an appropriate business model will require careful consideration of the following factors:

- **Sustainability/Financing.** Stakeholders should consider the overall estimated costs of the project, estimated volume and demand of digital public services, and the revenue-generating potential for the private sector. In general, PPP-type arrangements like BOTs and concessions offer the advantage of lower (or no) up-front costs for the government, which may enable those lacking investment and initial funding capability to deploy and sustain modern national digital identity systems. Nevertheless, they may not be appropriate for all types of projects.³⁸
- **Legal and ethical issues.** There may be risks associated with transferring management of the national identity system to a private company under certain partnership arrangements (for example, private ownership of public data may not be legal, advisable or socially acceptable). For example, according to a recent survey conducted by Accenture on behalf of GSMA, it is important for liability reasons for government to lead the delivery of civil registration systems, even though these can be facilitated by private sector entities.

38. See World Bank (2014) and World Bank (2009) for a more complete analysis of the potential benefits and risks of PPPs.

- **Government capacity.** All identity systems require significant government capacity. Even where governments are not building and managing identity systems in-house, they must clearly define the roles and responsibilities of different identity actors and provide the legal and regulatory framework to establish trust and protect privacy and personal data. For PPPs, special legislation may be required and strong governance practices are necessary to oversee project implementation and enforce regulations. In contrast, traditional public procurement projects involve well-known and often simpler contracts. However, projects where government officials are involved in operating identity systems—such as in public procurement— may require significant technical knowledge transfer.
- **Private sector activities.** The extent to which digital identity and authentication services are already commercially available and interoperable will dictate potential public and private sector use cases and cooperation. In any arrangement, stakeholders should structure contracts to help leverage private sector expertise and innovation to enable interoperability both at cross border and cross sector level. In PPPs, for example, private firms are paid based on output and thus able to design inputs to maximize efficiency.
- **Length of partnership.** One benefit to PPPs is the ability to capitalize on a long-term partnership. In some cases, however, there is a trade-off between the opportunities of a long-term contract and the ability of public actors to change suppliers when needed to avoid vendor or technology lock-in.



3 Common Principles for Unlocking the Value of Digital Identity

Advances in digital and biometric technology, combined with the already extensive use of mobile devices in the developing world offer a transformative solution to the global identity gap. In order to realize this potential, however, public and private sector stakeholders and development partners must collaborate in order to overcome the challenges to achieving digital identification that are described in Part I of this paper. This requires a sustained effort among actors, underpinned by common objectives and understanding. Building on a series of consultation forums, broad multi-stakeholder discussions, and previous research, we have identified three preliminary thematic areas to serve as the basis for principles of cooperation:

1. Universal Coverage. Identification management systems should strive for continuous universal coverage: officially recognized identification and authentication services should be accessible to all individuals from birth to death. Principles in this area could include:

- Non-discrimination and inclusivity
- Affordability
- Accessibility

2. Appropriate and Effective Design. Identity systems should be context appropriate and adaptable for long-term needs, including measures to ensure their demand, robustness, integrity

and resilience, interoperability, proportionality, vendor and technology neutrality, and fiscal and operational sustainability. Principles in this area could include:

- Prioritizing end-user needs and demands
- Integrity of systems
- Proportionality
- Open standards and outcomes-based approaches
- Long term financial sustainability

3. Building and Sustaining Trust. Identity systems must be built on a legal and operational foundation of trust and accountability between public agencies, private sector actors and individuals, who must be assured privacy and protection of their data, and the ability to exercise control and oversight over its use. Principles in this area could include

- The protection of privacy and security of data and users rights
- Strong accountability mechanisms
- Legal and trust frameworks supported by impartial adjudication

In order to **enable** the creation of identity systems that meet these standards, government and industry stakeholders must also develop a consensus regarding standards for (1) the legal and regulatory environment, (2) technology, (3) governance structures, (4) public-private cooperation, (5) stakeholder awareness, (6) convenience, and (7) facilitating a competitive market place.

At the time of publication, multi-stakeholder consultations were on-going to define and agree a set of principles. We recommend the continued development of these principles and enablers through an inclusive process so that they may be endorsed by a variety of stakeholders. Adhering to these principles will help align different actors, accelerate national identification strategies and enhance trust in the digital identity ecosystem for the benefit of governments, citizens, and the private sector.

Annex: Case Studies

Albania – eID and e-Passport

What is the project? In the early 2000s, Albania began its “Digital Albania” initiative in order to improve public and private service delivery. One of the goals of the initiative was to modernize the national identification system and begin issuing passports that complied with European standards. Identity became a priority in 2008, when the government needed to issue secure ID cards ahead of the 2009 elections. To implement this project, it awarded a concession to deliver 1.5 million eID cards to citizens. To date, some 3.2 million smartcards and 2.6 million biometric e-passports have been issued. In 2013, the concession was renewed for 10 years. These cards are used as voter ID in elections and for a variety of other services.

Who is involved? The Ministry of Interior Affairs is the main agency in charge of identification, although other public agencies were involved. The concession was awarded to Aleat, an Albanian subsidiary of Morpho and joint venture AAEF, which was created to manage the national identity project.

How does it work? Before this project, Albania’s national identity system included a number of paper-based registers across different provinces that were inherited from the Soviet era. Rather than attempting to digitize these records—many of which were inaccurate—the Ministry of Interior Affairs partnered with the private firm to re-register the entire population and create an entirely new, digital database. This was a full concession, and company implemented and managed every aspect of the project, including technology development, operation, and maintenance. In order to obtain an eID or passport, citizens enroll in one of 400 centers nation-wide, and their data is then validated against the central database. Cards are then printed off-site and sent back to the municipal enrollment center for later pick up. The private firm has added optional services to the process, including a fast-track system that allows citizens to get their passports within 24 hours or less for an extra fee. In addition, the smartcard includes digital certificates that can be used to access eGov services via kiosks. With the new passports, Albania reached an agreement with the European Commission in 2010 that allows Albanians the right to travel throughout the Schengen area without a visa.

Who collects and stores data? The private firm collects, manages, and stores all the data, and a copy of the data is provided to the Ministry of Interior Affairs. Although the firm technically owns the data, there are security measures in place to ensure that only Ministry officials can gain access to sensitive data.

How are investments and revenue divided? As a full concession, the firm incurs all design, building, and operational costs. The company collects the user-fees from the eIDs and e-passports, and pays the government a portion of these fees.

Chile – eID and e-Passport

What is the project? In 2013, Chile began a follow-on project as part of the process to modernize its national identification and passport systems. The goal was to strengthen and automate the registration and verification of citizens and foreign residents, increase the security of systems and documents, and comply with international standards for border crossing. In addition, the government sought to increase citizen's access to identification and passport services, particularly in remote areas. To implement this system, the government awarded a 10-year concession to a private firm to upgrade its national identity system and issue 25 million eID cards and 4 million e-passports by 2020.

Who is involved? The project was undertaken by the *Registro Civil e Identificación*, housed within the Ministry of Justice, which is in charge of civil registration and documentation for all Chileans and foreign residents. The main private sector partner for the provision of passports and the new ID cards is Morpho Chile. Sonda continues to provide the platform for civil registration.

How does it work? At the start of the concession, the private firm upgraded the *Registro's* existing technology platform—including hardware, software, and systems integration at the central database and the country's 900 enrollment stations—and also trained civil service staff on the use of the technology. Citizens enroll at one of the enrollment stations, and their data, including biometrics, is validated against the central database. The company then personalizes the eID smartcard or e-passport and sends it back to the enrollment station for the person to come and collect. The identity system uses a unique identifying number, RUN (*Rol Único Nacional*), which links the national ID, passport, and a number of other databases, such as the ministry of health and the ministry of social development. The connectivity of the registration process and integration with multiple databases has dramatically reduced enrollment time to only one hour. In addition, the biometric e-passport system has allowed Chile to become the first Latin American country to gain access to the US Visa Waiver program. With this system in place, Chile is now exploring expanded functionality for the smartcard, including digital signatures for authentication.

Who collects and stores data? All data is collected and stored by the *Registro Civil e Identificación*.

How are investments and revenue divided? The private firm invested significant capital to upgrade Chile's identity system. The *Registro Civil e Identificación* collects fees for issuing eID cards (around \$3,000 pesos or USD 4.50) and e-passports (around \$89,660 pesos or USD 134), and then pays the firm per document issued.

Estonia – Mobile eID

What is the project? Estonia's Mobile eID Solution (m-ID) was among the first of its kind and has been heralded as a model case internationally. The Government of Estonia has been offering services electronically through its eGovernance agenda since the early 2000s. Initially, the private sector was involved only in manufacturing smartcards, and online authentication was based on a PKI-enabled smartcard and a physical card reader with a USB hub. In 2007, a mobile operator began offering mobile authentication to facilitate e-banking transactions and other private-sector service exchanges. In 2011, the Government of Estonia reached an agreement with mobile operators to integrate this form of authentication into e-government services as well. Today, mobile ID can be used on most wireless devices for the entire range of government services, from tax returns to public transportation and voting in national elections.

Who is involved? The primary government body involved with m-ID is the Estonian Certification Authority, *Sertifitseerimiskeskus*, which manages the population registry. Other government agencies are responsible for the content and execution of electronic services. Private-sector partners include mobile operators EMT, Elisa, and Tele2.

How does it work? Users wishing to participate in the mobile ID scheme need to request special PKI-enabled SIM cards from their mobile operator. The user's identity is verified and a private key stored on the SIM card facilitates digital authentication through the mobile operator and a trusted service provider. These SIM cards are issued by the certification authority, but sold to customers by the respective operators as part of their existing mobile phone contract. To access an electronic service offered by the government through a mobile phone or a tablet, mobile ID offers secure digital two-factor identification without requiring additional hardware or documentation, such as a card reader.

Who collects and stores data? End user data is stored in the country's population registry, against which mobile operators will check their customer data in order to provide the authentication service. The mobile operator has no direct access to the registry or other citizen data; it merely sends a request to the government server and receives a positive or negative response.

How are investments and revenue divided? The technical infrastructure needed for a successful mobile ID environment was provided by the mobile operators. To some extent, the infrastructure was already in place by the time the Estonian government sought to introduce the m-ID project, as mobile identification was already established practice in the Estonian banking sector. The government provided no significant investment in mobile infrastructure. Mobile operators hope to recuperate the costs of investment through growing market shares by offering mobile ID to potential customers as well as end user charges for using the m-ID service. Pricing structures for mobile ID services vary depending on specific contract and bundling models, much like air time, data usage, or text messaging.

Finland – Mobile eID

What is the project? In Finland, multiple forms of electronic ID have existed since 2001. The banking sector had been demanding two-factor authentication involving a unique ID number, a PIN code, and a one-time password since the late 1980s. In terms of government-issued ID, Finland was the first country to roll out a national eID card in 1999. In 2008, in response to challenges of impracticality and underuse the existing systems were facing, a consortium of government agencies, mobile operators, and the Finnish Federation for Communications and Teleinformatics (FiCom) agreed to launch a mobile identification system that would combine the benefits of the existing systems and be more accessible to the public.

Who is involved? A number of public service and government agencies were involved in designing the terms for the mobile ID scheme, while the Finnish Population Register Centre (VRK) continues to be involved as the ultimate holder of population data. The system in itself was designed by three major mobile operators—DNA, Elisa, and TeliaSonera—and the PKI infrastructure had already been developed by the time that the mobile ID project was launched.

How does it work? The system is a two-way authentication system based on PKI SIM-cards and the operators' user database. When wishing to access an electronic service through a mobile phone, the user's phone number acts as a trigger for the mobile ID transaction – the user will only have to provide a PIN code to verify the correct use of his mobile device. User IDs are pre-identified, and a private key stored on the specialized SIM card facilitates the digital authentication through the mobile operator and a trusted service provider. What is distinctive about the Finnish mobile ID system is its inter-operability among mobile operators. Despite each provider operating its own mobile ID application, a so-called “circle of trust” agreement ensures that users will be able to access services through the application of a mobile operator other than their own.

Who collects and stores data? The VRK is the state Certificate Authority in the country. Prior to a change in legislation in 2009, it was the only entity able to issue unique identifiers to individuals. The authority still holds centralized population data for the country, which forms the basis for the national ID, but mobile operators are now able to issue Finnish unique identifiers to customers directly at the store, which will later be transmitted to the VRK database.

How are investments and revenue divided? The mobile ID project as a whole is largely built and owned by the private sector. As one of the most advanced mobile markets in the world, Finland benefited from high levels of network coverage, existing PKI infrastructure, and the large number of PKI-ready SIM cards already in circulation. No large investments in technology or infrastructure were required. Revenue is collected by the mobile operators on the basis of different pricing models agreed upon with service providers. Usage for consumers is initially free. Service providers who use mobile signature service are charged a set fee per transaction.

India – Aadhaar Unique ID

What is the project? In 2009, the Indian government embarked on an ambitious project to enroll its 1.2 billion people in a digital identity system that would provide each person with a unique identity number (Aadhaar) to serve as a foundation for proof of identity and public service delivery. The Unique Identification Authority of India (UIDAI) was created to design and manage this process. Rather than hiring thousands of staff and creating public-sector infrastructure to undertake this enrollment itself, UIDAI decided to rely on third parties to collect resident's data with the goal of increasing efficiency and value for money. To date, over 1 billion people have been registered (around two-thirds of these by private firms), and Aadhaar numbers have been linked to the delivery of Liquefied Petroleum Gas (LPG) subsidies, Public Distribution System rations, and other social protection programs. In the future, the goal is to connect Aadhaar to myriad other public and private services through a variety of partnerships.

Who is involved? The UIDAI is the main authority in charge of the Aadhaar program, while the “Registrars”—including state governments, public service agencies, banks, telecom companies, insurance agencies, etc.—sub-contract a variety of local agents to complete the registration process. Any public or private entity can then use the Aadhaar number to authenticate a user against the UIDAI database. The Standardization Testing and Quality Certification (STQC) Directorate is charged with ensuring that the technology meets UIDAI standards.

How does it work? UIDAI signs Memoranda of Understanding (MOUs) with Registrars in each state, and these Registrars may then contract with public entities or private companies to carry out the actual enrollment of residents according to UIDAI's strict technical specifications and regulations. The data captured by enrolling agencies—including biographical information such as name, gender, date of birth, and address, along with 10 fingerprints, two iris scans and a photo—are then securely sent to UIDAI for verification and de-duplication. Once the digital identity is verified, a unique identification number (the Aadhaar number) is issued to the enrollee, who receives a printed letter with the number in the mail. Public and private service providers can then authenticate identity online using the Aadhaar number and a fingerprint (e.g., via a point-of-sale or POS device). Vodafone, for example, has partnered with the Indian Telecom Authority to begin Aadhaar-based e-KYC verification of new customers in Kolkata.

Who collects and stores data? The enrolling agents collect the data, which is then encrypted and sent to UIDAI for validation against its central database. When Aadhaar is used for authentication, service providers simply send a request to UIDAI for verification of an identity (“is this person who she claims to be?”) and receive a yes/no response in return—data remain with UIDAI and are not shared or accessible by other public or private entities.

How are investments and revenue divided? All costs for establishing registration infrastructure are borne by the enrolling agents; the UIDAI only provides the technical standards that they must meet. Enrollment in Aadhaar is free, and no revenue is generated by user-fees (although certain agents may charge user fees for add-on services). The government pays enrolling agents based on the number of people enrolled, at a standard rate of INR 31 (USD 0.467) per person—to date, this amounts to approximately USD 311 million in profit for these firms.

Moldova – Mobile eID

What is the project? The Moldova Mobile e-ID Solution (Me-ID) was developed in 2011 by the Government of Moldova as part of an e-Governance program aimed at facilitating and digitalizing public service delivery. After a cost-benefit review examining various models and scenarios, the government decided in 2011 to launch a client-side mobile ID system based on PKI-enabled SIM cards that would allow for digital authentication of citizens accessing public services electronically. Although certain government agencies had already built a PKI-infrastructure, the project team decided to partner with the private sector in order to improve accessibility for citizens and foster long-term innovation and investment in electronic services.

Who is involved? The e-Government office within the State Chancellery acts as the national certification authority for digital identity and as a coordinating body for the shift towards e-Governance. On the private-sector side, the firms involved are the country's leading mobile operators, MoldCell/TeliaSonera and Orange.

How does it work? As the Moldovan Me-ID project was closely modeled on the Estonian system, the technical application is very similar in its details. Users wishing to participate in the mobile ID scheme request special PKI SIM cards from their mobile operator. These SIM cards are issued by the certification authority, but sold to customers by the respective operators as part of their existing mobile phone contract. When accessing electronic services offered by the government through a mobile phone or a tablet, mobile ID offers secure digital two-factor identification without requiring additional hardware or documentation. The users ID will have been pre-identified, and a private key stored on the specialized SIM card facilitates the digital authentication through the mobile operator and a trusted service provider.

Who collects and stores data? End user data is stored in the country's population registry, against which mobile operators will check their customer data in order to provide the authentication service. The mobile operator has no direct access to the registry or other citizen data; it merely sends a request to the government server and receives a positive or negative response. Mobile operators will have records of customers' use of mobile signatures, but no information regarding the exact nature of services for which the mobile signatures were used.

How are investments and revenue divided? The technical infrastructure needed for a successful mobile ID environment was provided by the mobile operators. While mobile phone penetration was already high in Moldova by the time the Me-ID project was rolled out, the specific nature of the PKI authentication system required additional investments in hardware and network strength. The cost for these investments (around EUR 400-500k) was borne almost entirely by the mobile operators; the government spent approximately 30k to connect the infrastructure. Mobile operators charge end-users a fee for the use of mobile signatures and pass on part of the income to the government as part of a revenue-sharing agreement. Pricing structures for mobile ID services vary depending on specific contract and bundling models, much like air time, data usage, or text messaging.

Nigeria – National eID

What is the project? In 2007, the Nigerian Identity Management Commission (NIMC) was tasked with creating a new National Identity Database built around the issuance of unique National Identity Numbers (NINs) and a multi-purpose smartcard. The goal of the new system is to streamline Nigeria's existing ecosystem of multiple identity systems in the country. In order to stimulate use of the ID card, the NIMC has begun offering networked financial services as one application on its smartcard. Since 2013, it has been partnering with MasterCard, Visa, and Verve, a local payment network. In separate agreements with local banks, these cards can be linked to pre-paid bank accounts and can be used to pay for goods and services. Eventually, a variety of databases and services may be linked to a single-platform eID, including the including driver's licenses, voter registration, health insurance, taxes, SIM card registration, and pensions.

Who is involved? The NIMC is responsible for enrollment, verification, and issuance of the smartcards. MasterCard, Visa, and Verve are the payments technology providers, Unified Payment Services Limited is the payments processor, and a number of banks (including Access Bank Plc, United Bank for Africa, Union Bank, etc.) are providing the pre-paid accounts. The Central Bank of Nigeria and other agencies are involved in an effort to offer bank verification numbers (BVNs), extend connectivity and the number of payment terminals around the country.

How does it work? Once a person is registered in the National Identity Database by the NIMC, they collect their card at an NIMC enrollment center and chose a PIN number to access their pre-paid account (card-holders should also be able to link existing bank accounts to their card). They can then use the cards to deposit or withdraw cash and make payments to any entity or merchant that accepts the cards in Nigeria or abroad. The goal is also to include online and offline authentication services using biometrics and the embedded chip via a POS device. Future rounds of ID cards may include service agreements with other companies following a similar design.

Who collects and stores data? The NIMC collects, validates, and stores all personal and biometric data for the National Identity Database. The private firms cannot access this data.

How are investments and revenue divided? The NIMC contracted suppliers to provide smartcards under a normal public procurement process. As such, the funding for the eID system infrastructure is provided by the government. However, the influx of millions of new smartcard users incentivizes the companies to extend their network within the country.

References

- Asian Development Bank (ADB), Inter-American Development Bank (IDB), World Bank Group. (2014). "Public-Private Partnerships Reference Guide: Version 2.0. Retrieved from <http://api.ning.com/files/lumatxxOjz3owSB05xZDkmWIE7GTVYA3cXwt4K4s3UyONTppRgPWYO1LrWaTUqybQeTXleuSYUxbPFWlyusyNI5rL6b2Ms/PPReferenceGuidev02Web.pdf>."
- Banerjee, S. 2015. "From Cash to Digital Transfers in India: The Story So Far." CGAP Brief, February 2015, Consultative Group to Assist the Poor (CGAP) Washington, DC. http://www.cgap.org/sites/default/files/Brief-From-Cash-to-Digital-Transfers-in-India-Feb-2015_0.pdf.
- Barnwal, P. 2015. "Curbing Leakage in Public Programs with Biometric Identification Systems: Evidence from India's Fuel Subsidies. Job Market Paper, School of International and Public Affairs, Columbia University, New York. <http://www.columbia.edu/~pb2442/subsidyLeakageUID.pdf>".
- Boston Consulting Group, 2013. "The Value of Our Digital Identity" study, 2013. Retrieved from <http://www.libertyglobal.com/pdf/public-policy/the-value-of-our-digital-identity.pdf>.
- Dahan M., A. Gelb. 2015. "Role of Identification in the Post-2015 Development Agenda, Working Paper, World Bank and Center for Global Development, Washington, DC."
- Dahan M., L Hanmer. 2015. The Identification for Development (ID4D) Agenda: Its Potential for Empowering Women and Girls. World Bank, Washington, DC.
- Dahan M., R. Sudan. 2015. "Digital ID for Development, Working Paper, Connections Note #18, World Bank, Washington, DC."
- Dunning, C., A. Gelb, and S. Raghavan. 2014. "Birth Registration, Legal Identity, and the Post-2015 Agenda. Policy Paper 46, Center for Global Development, Washington, DC."
- Gelb, A., J. Clark. 2013. "Identification for Development: The Biometrics Revolution." Center for Global Development Working Paper no. 315.
- Gelb, A. and Diofasi, A. 2015. "Scoping Paper on Identification and Development. Center for Global Development".
- Gelb, A., and Diofasi, A. 2016. "Using Identification for Development: Some Guiding Principles". CGD Notes.
- Global Findex database: <http://www.worldbank.org/en/programs/globalfindex>.
- GSMA, 2015. "Mobile Identity Regulatory Overview (second edition)", Report, 2015. Retrieved from <http://www.gsma.com/personaldata/wp-content/uploads/2015/01/Personal-Data-Regulatory-Overview-2014.pdf>
- GSMA and SIA joint publication, 2014. "Mobile Identity – Unlocking the Value of Digital Economy", White Paper, 2014. Retrieved from http://www.gsma.com/personaldata/wp-content/uploads/2014/10/14-10-10-GSMA-SIA-Joint-Paper-Mobile-Identity_October-2014.pdf
- GSMA case studies: Finnish Mobile ID: A Lesson in Interoperability; Estonia's Mobile-ID: Driving Today's e-Services Economy; Norwegian Mobile Bank ID: Reaching Scale through Collaboration; Swisscom Mobile ID: Enabling an Ecosystem for Secure Mobile Authentication; Mobile Signature in Turkey – A Case Study of Turkcell; Mobilimza; Mobile Birth Registration in Sub-Saharan Africa: A case study of Orange Senegal and Uganda Telecom solutions; Retrieved from <http://www.gsma.com/newsroom/gsmadocuments/>
- Harbitz, M. and Kentala, K., 2015. "Dictionary for Civil Registration and Identification". IDB Working Paper, 2015.
- World Bank. 2009. Public-Private Partnerships in E-Government: Knowledge Map. Prepared by the Institute for Public-Private Partnerships. Washington, DC. Retrieved from http://www.infodev.org/infodev-files/resource/InfodevDocuments_821.pdf
- Malik, T. 2014. "Technology in the Service of Development: The NADRA Story." Retrieved from <http://www.cgdev.org/publication/technology-servicedevelopment-nadra-story>
- SIA, 2013. "eGov study", 2013. Retrieved from <https://www.secureidentityalliance.org/index.php/news-events/news/168-trusted-identity-egovernment>
- SIA, 2015. "Civil Registry Consolidation through Digital Identity Management" report. Retrieved from <https://www.secureidentityalliance.org/index.php/news-events/news/325-new-civil-registry-and-identity-guidance-for-governments>
- The Economist. 2014. "Digital Identity Cards: Estonia takes the plunge." Retrieved from The Economist <http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estoniatakes-plunge> (June 28)
- World Bank, 2014a. "Digital Identity Toolkit", Working Paper, Washington DC. Retrieved from <http://documents.worldbank.org/curated/en/2014/06/20272197/digital-identity-toolkit-guide-stakeholders-africa>
- World Bank. 2014b. Public-Private Partnerships Reference Guide, Version 2.0. Washington DC. Retrieved from <https://library.pppknowledgelab.org/Knowledge%20Lab/documents/2480>
- World Bank, 2015a. "ID4D Integration Approach Study", Working Paper, Washington DC. Retrieved from http://imagebank.worldbank.org/servlet/WDSContentServer/IW3P/IB/2015/09/21/090224b0830efe0f/2_0/Rendered/PDF/IdentificationOationOapproachOstudy.pdf
- World Bank, 2015b. "Analysis of Existing eGovernment and Trade Facilitation Public Private Partnerships (PPPs) Worldwide", Internal World Bank Group Working Paper, Washington DC.
- World Bank, 2016. "Identification for Development Strategic Framework", Working Paper, Washington DC.



www.gsma.com/digitalidentity

www.worldbank.org/en/programs/id4d

www.secureidentityalliance.org

